APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/561,207	11/03/2006	Jorge Cuellar		4069

7590 08/31/2007	EXAMINER
JORGE CUELLAR	LAFORGIA, CHRISTIAN A
HOLLRIEGELSKREUTHER WEG 14	
BAIERBRUNN, 82065	
GERMANY	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/561,207	CUELLAR ET AL.
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *12/19/05*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-14 have been presented for examination.

Priority

2.   Acknowledgment is made of applicant's claim for foreign priority.

Information Disclosure Statement

3.   The information disclosure statement (IDS) submitted on 19 December 2005 is in

compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the

information disclosure statement.

Drawings

4.   Figure 1 should be designated by a legend such as --Prior Art-- because only that which is

old is illustrated according to page 13, lines 23-24 of the Specification. See MPEP § 608.02(g).

Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office

action to avoid abandonment of the application. The replacement sheet(s) should be labeled

"Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion

of the drawing figures. If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The objection

to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

5.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

6.   Claims 13 and 14 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. The Applicant fails to set forth any particular structure

in the specification to support the "key generation unit," the "encryption unit," and the

"decryption unit." The Applicant states at page 7, lines 8-10 that the components of the

invention can be produced in the form of software or by means of a computer program, which

renders claims 13 and 14, given their broadest reasonable interpretation while keeping the

specification in mind, computer programs *per se*. Since the computer program is not embodied

on a computer storage medium, or something of the like, and there is no structure disclosed,

claims 13 and 14 are drawn to nonstatutory subject matter.

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 1-10 and 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S.

Patent Application Publication No. 2004/0093522 A1 to Bruestle et al., hereinafter Bruestle.

9.   As per claim 1, Bruestle teaches a method for forming an encrypted message including

communication configuration data, comprising:

executing an Internet-based authentication method using at least one service from a unit

in a security layer or link control layer between a first communication unit and a second

communication unit (Figures 2 [elements 101-106], 3 [elements 201-202], paragraphs 0005,

0008, 0013, 0018, i.e. i.e. extensible authentication protocol), so that at least one pair of

cryptographic keys is formed for the first communication unit and for the second communication

unit (paragraphs 0005, 0012, 0028, i.e. EAP-TLS generates user and session-based encryption

keys that are distributed to the client and the access point to secure the connection), and

encrypting the communication configuration data of the first communication unit using at

least one cryptographic key of the at least one pair of cryptographic keys, thus forming the

encrypted message (paragraphs 0012, 0021-0024, i.e. client and access point share keying

information used to encrypt data traffic between them, including access control parameters and

access privileges).

10.   Regarding claim 2, Bruestle teaches wherein the Internet-based authentication method is

based on an extensible authentication protocol method (Figures 2 [elements 101-106], 3

[elements 201-202], paragraphs 0005, 0008, 0013, 0018, i.e. i.e. extensible authentication

protocol).

11.   Regarding claim 3, Bruestle teaches the communication configuration data is transmitted

from the first communication unit to the second communication unit by using electronic

messages according to the Internet-based authentication method (paragraphs 0021-0024).

12.   Regarding claim 4, Bruestle teaches wherein the communication configuration data is

transmitted from the first communication unit to the second communication unit by using

electronic messages according to one of the following Internet-based authentication methods:

    • protected extensible authentication protocol method (paragraph 0013, i.e. PEAP),

    • extensible authentication protocol tunneled TLS authentication protocol method

(paragraph 0013, i.e. EAP TTLS), or

    • protocol for carrying authentication for network access method (paragraph 0013).

13.   Regarding claim 5, Bruestle teaches wherein the first communication unit is a

communication unit of a communication network element (Figures 1 [elements 12, 13, 14], 2

[elements 12, 14, 16], 3 [elements 12, 15, 16], paragraphs 0021, 0029).

14.   With regards to claim 6, Bruestle teaches wherein the first communication unit is a

communication unit of a communication network element in a mobile radio communication

network (paragraphs 0019, 0024, i.e. IEEE 802.11b is a wireless radio network).

15.   Regarding claims 7 and 8, Bruestle teaches wherein the second communication unit is a

communication terminal (Figures 1-3 [element 10], paragraph 0019), wherein the second

communication unit is a mobile radio communication terminal (paragraphs 0019, 0024, i.e. using

802.11b to access wireless networks).

16.   Regarding claims 9 and 10, Bruestle teaches wherein the communication configuration

data is encoded according to a protocol format of a protocol for configuring a communication

terminal, wherein the communication configuration data is encoded according to a protocol

format of a protocol for dynamically configuring a communication terminal (Figure 3 [elements

206, 207], paragraph 0032, i.e. RADIUS).

17.   As per claim 12, Bruestle teaches a method for encrypting an encrypted message

including communication configuration data, comprising:

executing an Internet-based authentication using at least one service from a unit in a

security layer or link control layer between a first communication unit and a second

communication unit (Figures 2 [elements 101-106], 3 [elements 201-202], paragraphs 0005,

0008, 0013, 0018, i.e. i.e. extensible authentication protocol), so that at least one pair of

cryptographic keys is formed for the first communication unit and for the second communication

unit (paragraphs 0005, 0012, 0028, i.e. EAP-TLS generates user and session-based encryption

keys that are distributed to the client and the access point to secure the connection), and

determining communication configuration data of the second communication unit using

at least one cryptographic key of the at least one pair of cryptographic keys to decrypt the

encrypted message including the communication configuration data (Figure 3 [elements 206,

207], paragraphs 0012, 0021-0024, i.e. client and access point share keying information used to

encrypt data traffic between them, including access control parameters and access privileges; to

accept the access parameters associated with the RADIUS set-up the client workstation would

have to decrypt the information).

18.   As per claim 13, Bruestle teaches a device for forming an encrypted message, the

encrypted message including communication configuration data, comprising:

a key generation unit (paragraphs 0005, 0012, 0028, i.e. generate user- and session-based

encryption keys) configured to execute an Internet-based authentication method using at least

one service from a unit in a security layer between a first communication unit and a second

communication unit (Figures 2 [elements 101-106], 3 [elements 201-202], paragraphs 0005,

0008, 0013, 0018, i.e. i.e. extensible authentication protocol), so that at least one pair of

cryptographic keys is formed for the first communication unit and for the second communication

unit (paragraphs 0005, 0012, 0028, i.e. EAP-TLS generates user and session-based encryption

keys that are distributed to the client and the access point to secure the connection); and

an encryption unit configured to encrypt the communication configuration data by using

at least one cryptographic key of the at least one pair of cryptographic keys, forming the

encrypted message (paragraphs 0012, 0021-0024, i.e. client and access point share keying

information used to encrypt data traffic between them, including access control parameters and

access privileges).

19.   As per claim 14, Bruestle teaches a device for encrypting an encrypted message, the

encrypted message containing including communication configuration data, comprising:

a key generation unit (paragraphs 0005, 0012, 0028, i.e. generate user- and session-based

encryption keys) configured to execute an Internet-based authentication method-by using at least

one service from a unit in a security layer between a first communication unit and a second

communication unit (Figures 2 [elements 101-106], 3 [elements 201-202], paragraphs 0005,

0008, 0013, 0018, i.e. i.e. extensible authentication protocol), so that at least one pair of

cryptographic keys is formed for the first communication unit and for the second communication

unit (paragraphs 0005, 0012, 0028, i.e. EAP-TLS generates user and session-based encryption

keys that are distributed to the client and the access point to secure the connection), and

a decryption unit configured to decrypt the communication configuration data of the

second communication unit by using at least one cryptographic key of the at least one pair of

cryptographic keys in decrypting the encrypted message including the communication

configuration data (Figure 3 [elements 206, 207], paragraphs 0012, 0021-0024, i.e. client and

access point share keying information used to encrypt data traffic between them, including

access control parameters and access privileges; to accept the access parameters associated with

the RADIUS set-up the client workstation would have to decrypt the information).

Claim Rejections - 35 USC § 103

20.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

21.   Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bruestle in view

of "Using RADIUS backend for DHCP over IKE," by T. Kivinen, hereinafter Kivinen.

22.   Concerning claim 11, Bruestle does not teach wherein the communication configuration

data is encoded according to a dynamic host configuration protocol for dynamically configuring

a communication terminal.

23.   Kivinen teaches combining DHCP functions with the RADIUS attributes (**Section 2.**

Using RADIUS backend).

24.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to include communication configuration data encoded according to a dynamic host

configuration protocol for dynamically configuring a communication terminal, since Kivinen

states in **Section 5. "Security Consideration"** that the connection between the gateway and the

RADIUS server might be vulnerable to attack, and should be protected by using a protocol such as EAP.

Conclusion

25.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

26.   The following patents are cited to further show the state of the art with respect to the extensible authentication protocol, such as:

United States Patent Application Publication No. 2003/0084287 A1 to Wang et al., which is cited to show authenticating a roaming device using EAP.

United States Patent Application Publication No. 2004/0034771 A1 to Edgett et al., which is cited to show updating or changing security information in overlapping periods.

United States Patent Application Publication No. 2002/0174335 A1 to Zhang et al., which is cited to show an IP-based authentication, accounting, and authorization scheme for virtual wireless local area networks.

United States Patent Application Publication No. 2005/0021979 A1 to Wiedmann et al., which is cited to show remote authentication using EAP.

27.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

28.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

29.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf